MIMO Gaussian Broadcast Channels with Confidential and Common Messages

Ruoheng Liu, Tie Liu, H. Vincent Poor, and Shlomo Shamai (Shitz)

***Abstract*—This paper considers the problem of secret communication over a two-receiver multiple-input multiple-output (MIMO) Gaussian broadcast channel. The transmitter has two independent, confidential messages and a common message. Each of the confidential messages is intended for one of the receivers but needs to be kept perfectly secret from the other, and the common message is intended for both receivers. It is shown that a natural scheme that combines secret dirty-paper coding with Gaussian superposition coding achieves the secrecy capacity region. To prove this result, a channel-enhancement approach and an extremal entropy inequality of Weingarten *et al.* are used.**

I. Introduction

In this paper, we study the problem of secret communication over a multiple-input multiple-output (MIMO) Gaussian broadcast channel with two receivers. The transmitter is equipped with t transmit antennas, and receiver k, $k = 1, 2$, is equipped with r_k receive antennas. A discrete-time sample of the channel at time m can be written as

$$\mathbf{Y}_k[m] = \mathbf{H}_k \mathbf{X}[m] + \mathbf{Z}_k[m], \quad k = 1, 2 \tag{1}$$

where $\mathbf{H}_k$ is the (real) channel matrix of size $r_k \times t$, and $\{\mathbf{Z}_k[m]\}_m$ is an independent and identically distributed (i.i.d.) additive vector Gaussian noise process with zero mean and identity covariance matrix. The channel input $\{\mathbf{X}[m]\}_m$ is subject to the matrix power constraint:

$$\frac{1}{n}\sum_{m=1}^{n}\left(\mathbf{X}[m]\mathbf{X}^{\mathsf{T}}[m]\right) \preceq \mathbf{S} \tag{2}$$

where $\mathbf{S}$ is a positive semidefinite matrix, and "$\preceq$" denotes "less than or equal to" in the positive semidefinite partial ordering between real symmetric matrices. Note that (2) is a rather general power constraint that subsumes many other important power constraints including the average total and per-antenna power constraints as special cases.

This research was supported by the United States National Science Foundation under Grant CNS-09-05398, CCF-08-45848 and CCF-09-16867, by the Air Force Office of Scientific Research under Grant FA9550-08-1-0480, by the European Commission in the framework of the FP7 Network of Excellence in Wireless Communications NEWCOM++, and by the Israel Science Foundation.

Ruoheng Liu and H. Vincent Poor are with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA (e-mail: {rliu,poor}@princeton.edu).

Tie Liu is with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843, USA (e-mail: tieliu@tamu.edu).

Shlomo Shamai (Shitz) is with the Department of Electrical Engineering, Technion-Israel Institute of Technology, Technion City, Haifa 32000, Israel (e-mail: sshlomo@ee.technion.ac.il).

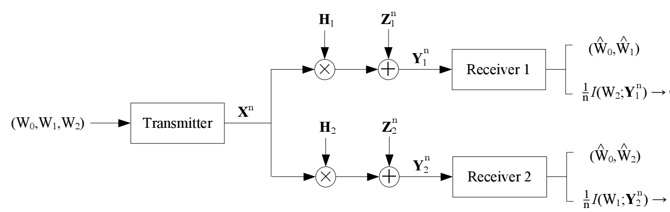

Fig. 1. Channel model

As shown in Fig. 1, we consider the communication scenario in which there is a common message W_0 and two independent, confidential messages W_1 and W_2 at the transmitter. Message W_0 is intended for both receivers. Message W_1 is intended for receiver 1 but needs to be kept secret from receiver 2, and message W_2 is intended for receiver 1 but needs to be kept secret from receiver 2. The confidentiality of the messages at the unintended receivers is measured using the normalized information-theoretic criteria [1]

$$\frac{1}{n}I(W_1;\mathbf{Y}_2^n) \to 0 \quad \text{and} \quad \frac{1}{n}I(W_2;\mathbf{Y}_1^n) \to 0 \tag{3}$$

where $\mathbf{Y}_k^n := (\mathbf{Y}_k[1], \ldots, \mathbf{Y}_k[n])$, $k = 1, 2$, and the limits are taken as the block length $n \to \infty$. The goal is to characterize the *entire* secrecy rate region $\mathcal{C}_s^{[\mathrm{SBC}]}(\mathbf{H}_1, \mathbf{H}_2, \mathbf{S}) = \{(R_0, R_1, R_2)\}$ that can be achieved by any coding scheme, where R_0, R_1 and R_2 are the communication rates corresponding to the common message W_0, the confidential message W_1 destined for receiver 1 and the confidential message W_2 destined for receiver 2, respectively.

In recent years, MIMO secret communication has been an active area of research. Several *special* cases of the communication problem that we consider here have been studied in the literature. Specifically,

- With only one confidential message (W_1 or W_2), the problem was studied as the MIMO Gaussian wiretap channel. The secrecy capacity of the MIMO Gaussian wiretap channel was characterized in [2] and [3] under the matrix power constraint (2) and in [4] and [5] under an average total power constraint.
- With both confidential messages W_1 and W_2 but *without* the common message W_0, the problem was studied in [6] for the multiple-input single-output (MISO) case and in [7] for general MIMO case. Rather surprisingly, it was shown in [7] that, under the matrix power constraint (2), both confidential messages can be *simultaneously* communicated at their respected maximum secrecy rates.

- With only one confidential message (W_1 or W_2) *and* the common message W_0, the secrecy capacity region of the channel was characterized in [8] using a channel-enhancement approach [9] and an extremal entropy inequality of Weingarten *et al.* [10].

The main contribution of this paper is to provide a precise characterization of the secrecy capacity region of the MIMO Gaussian broadcast channel with a more complete message set that includes a common message W_0 and two independent, confidential messages W_1 and W_2 by generalizing the channel-enhancement argument of [8].

II. Main Result

The main result of the paper is summarized in the following theorem.

Theorem 1 (General MIMO Gaussian broadcast channel): The secrecy capacity region of the MIMO Gaussian broadcast channel (1) with a common message W_0 (intended for both receivers) and confidential messages W_1 (intended for receiver 1 but needing to be kept secret from receiver 2) and W_2 (intended for receiver 2 but needing to be kept secret from receiver 1) under the matrix power constraint (2) is given by the set of nonnegative rate triples (R_0, R_1, R_2) such that

$$\begin{aligned} R_0 \le \min\Bigg\{&\frac{1}{2}\log\left|\frac{\mathbf{H}_1\mathbf{S}\mathbf{H}_1^{\intercal}+\mathbf{I}_{r1}}{\mathbf{H}_1(\mathbf{S}-\mathbf{B}_0)\mathbf{H}_1^{\intercal}+\mathbf{I}_{r1}}\right|,\\ &\frac{1}{2}\log\left|\frac{\mathbf{H}_2\mathbf{S}\mathbf{H}_2^{\intercal}+\mathbf{I}_{r2}}{\mathbf{H}_2(\mathbf{S}-\mathbf{B}_0)\mathbf{H}_2^{\intercal}+\mathbf{I}_{r2}}\right|\Bigg\}\\ R_1 \le &\frac{1}{2}\log\left|\mathbf{I}_{r_1}+\mathbf{H}_1\mathbf{B}_1\mathbf{H}_1^{\intercal}\right|\\ &-\frac{1}{2}\log\left|\mathbf{I}_{r_2}+\mathbf{H}_2\mathbf{B}_1\mathbf{H}_2^{\intercal}\right|\\ \text{and}\qquad R_2 \le &\frac{1}{2}\log\left|\frac{\mathbf{I}_{r_2}+\mathbf{H}_2(\mathbf{S}-\mathbf{B}_0)\mathbf{H}_2^{\intercal}}{\mathbf{I}_{r_2}+\mathbf{H}_2\mathbf{B}_1\mathbf{H}_2^{\intercal}}\right|\\ &-\frac{1}{2}\log\left|\frac{\mathbf{I}_{r_1}+\mathbf{H}_1(\mathbf{S}-\mathbf{B}_0)\mathbf{H}_1^{\intercal}}{\mathbf{I}_{r_1}+\mathbf{H}_1\mathbf{B}_1\mathbf{H}_1^{\intercal}}\right| \end{aligned} \tag{4}$$

for some $\mathbf{B}_0 \succeq 0$, $\mathbf{B}_1 \succeq 0$ and $\mathbf{B}_0+\mathbf{B}_1 \preceq \mathbf{S}$. Here, $\mathbf{I}_{r_k}$ denotes the identity matrix of size $r_k \times r_k$ for $k = 1, 2$.

Remark 1: Note that for any given $\mathbf{B}_0$, the upper bounds on R_1 and R_2 can be simultaneously maximized by a same $\mathbf{B}_1$. In fact, the upper bounds on R_1 and R_2 are fully symmetric with respect to $\mathbf{H}_1$ and $\mathbf{H}_2$, even though it is not immediately evident from the expressions themselves.

To prove Theorem 1, we shall follow [9] and first consider the *canonical* aligned case. In an *aligned* MIMO Gaussian broadcast channel [9], the channel matrices $\mathbf{H}_1$ and $\mathbf{H}_2$ are square and invertible. Multiplying both sides of (1) by $\mathbf{H}_k^{-1}$, the channel can be equivalently written as

$$\mathbf{Y}_k[m] = \mathbf{X}_k[m] + \mathbf{Z}_k[m], \quad k = 1, 2 \tag{5}$$

where $\{\mathbf{Z}_k[m]\}_m$ is an i.i.d. additive vector Gaussian noise process with zero mean and covariance matrix $\mathbf{N}_k = \mathbf{H}_k^{-1}\mathbf{H}_k^{-\intercal}$, $k = 1, 2$. The secrecy capacity region of the aligned MIMO Gaussian broadcast channel is summarized in the following theorem.

Theorem 2 (Aligned MIMO Gaussian broadcast channel): The secrecy capacity region $\mathcal{C}_s^{[\mathrm{SBC}]}(\mathbf{N}_1, \mathbf{N}_2, \mathbf{S})$ of the aligned MIMO Gaussian broadcast channel (5) with a common message W_0 and confidential messages W_1 and W_2 under the matrix power constraint (2) is given by the set of nonnegative rate triples (R_0, R_1, R_2) such that

$$\begin{aligned} R_0 &\le \min\left\{\frac{1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_1}{(\mathbf{S}-\mathbf{B}_0)+\mathbf{N}_1}\right|, \frac{1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_2}{(\mathbf{S}-\mathbf{B}_0)+\mathbf{N}_2}\right|\right\}\\ R_1 &\le \frac{1}{2}\log\left|\frac{\mathbf{B}_1+\mathbf{N}_1}{\mathbf{N}_1}\right| - \frac{1}{2}\log\left|\frac{\mathbf{B}_1+\mathbf{N}_2}{\mathbf{N}_2}\right|\\ R_2 &\le \frac{1}{2}\log\left|\frac{(\mathbf{S}-\mathbf{B}_0)+\mathbf{N}_2}{\mathbf{B}_1+\mathbf{N}_2}\right| - \frac{1}{2}\log\left|\frac{(\mathbf{S}-\mathbf{B}_0)+\mathbf{N}_1}{\mathbf{B}_1+\mathbf{N}_1}\right| \end{aligned} \tag{6}$$

for some $\mathbf{B}_0 \succeq 0$, $\mathbf{B}_1 \succeq 0$ and $\mathbf{B}_0+\mathbf{B}_1 \preceq \mathbf{S}$.

Next, we prove Theorem 2 by generalizing the channel-enhancement argument of [8]. Extension from the aligned case (6) to the general case (4) follows from the standard limiting argument [9]; the details are deferred to the extended version of this work [11].

III. Proof of Theorem 2

A. Achievability

The problem of a two-receiver discrete memoryless broadcast channel with a common message and two confidential common messages was studied in [12], where an achievable secrecy rate region was given by the set of rate triples (R_0, R_1, R_2) such that

$$\begin{aligned} &R_0 \le \min[I(\mathbf{U}_0;\mathbf{Y}_1),\ I(\mathbf{U}_0,\mathbf{Y}_2)]\\ &R_1 \le I(\mathbf{V}_1;\mathbf{Y}_1|\mathbf{U}_0) - I(\mathbf{V}_1;\mathbf{V}_2,\mathbf{Y}_2|\mathbf{U}_0)\\ \text{and}\qquad &R_2 \le I(\mathbf{V}_2;\mathbf{Y}_2|\mathbf{U}_0) - I(\mathbf{V}_2;\mathbf{V}_1,\mathbf{Y}_1|\mathbf{U}_0) \end{aligned} \tag{7}$$

where $\mathbf{U}_0$, $\mathbf{V}_1$ and $\mathbf{V}_2$ are auxiliary random variables such that $(\mathbf{U}_0, \mathbf{V}_1, \mathbf{V}_2) \to \mathbf{X} \to (\mathbf{Y}_1, \mathbf{Y}_2)$ forms a Markov chain. The scheme to achieve this secrecy rate region is a natural combination of secret dirty-paper coding and superposition coding. Thus, the achievability of the secrecy rate region (6) follows from that of (7) by setting

$$\begin{aligned} \mathbf{V}_1 &= \mathbf{U}_1 + \mathbf{F}\mathbf{U}_2\\ \mathbf{V}_2 &= \mathbf{U}_2\\ \text{and}\quad \mathbf{X} &= \mathbf{U}_0 + \mathbf{U}_1 + \mathbf{U}_2 \end{aligned}$$

where $\mathbf{U}_0$, $\mathbf{U}_1$ and $\mathbf{U}_2$ are three independent Gaussian vectors with zero means and covariance matrices $\mathbf{B}_0$, $\mathbf{B}_1$ and $\mathbf{S}-\mathbf{B}_0-\mathbf{B}_1$, respectively, and

$$\mathbf{F} := \mathbf{B}\mathbf{H}_1^{\intercal}(\mathbf{I}_{r_1} + \mathbf{H}_1\mathbf{B}\mathbf{H}_1^{\intercal})^{-1}\mathbf{H}_1.$$

The details of the proof are deferred to the extended version of this work [11].

B. The converse

Next, we prove the converse part of Theorem 2 assuming that $\mathbf{S} \succ 0$. The case where $\mathbf{S} \succeq 0$, $|\mathbf{S}| = 0$ can be found in the extended version of this work [11].

Let

$$f_0(\mathbf{B}_0) = \min\left\{\frac{1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_1}{(\mathbf{S}-\mathbf{B}_0)+\mathbf{N}_1}\right|, \frac{1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_2}{(\mathbf{S}-\mathbf{B}_0)+\mathbf{N}_2}\right|\right\}$$

$$f_1(\mathbf{B}_1) = \frac{1}{2}\log\left|\frac{\mathbf{B}_1+\mathbf{N}_1}{\mathbf{N}_1}\right| - \frac{1}{2}\log\left|\frac{\mathbf{B}_1+\mathbf{N}_2}{\mathbf{N}_2}\right|$$

and
$$f_2(\mathbf{B}_0,\mathbf{B}_1) = \frac{1}{2}\log\left|\frac{(\mathbf{S}-\mathbf{B}_0)+\mathbf{N}_2}{\mathbf{B}_1+\mathbf{N}_2}\right| - \frac{1}{2}\log\left|\frac{(\mathbf{S}-\mathbf{B}_0)+\mathbf{N}_1}{\mathbf{B}_1+\mathbf{N}_1}\right|. \tag{8}$$

Then, the secrecy rate region (6) can be rewritten as

$$\mathcal{R}_{in} := \bigcup_{\mathbf{B}_0\succeq 0, \mathbf{B}_1\succeq 0, \mathbf{B}_0+\mathbf{B}_1\preceq \mathbf{S}} \Big\{(R_0,R_1,R_2)\Big| R_0 \le f_0(\mathbf{B}_0),\ R_1 \le f_1(\mathbf{B}_1),\ R_2 \le f_2(\mathbf{B}_0,\mathbf{B}_1)\ \Big\}. \tag{9}$$

To show that $\mathcal{R}_{in}$ is indeed the secrecy capacity region of the aligned MIMO Gaussian broadcast channel (5), we will consider proof by contradiction. Assume that $(R_0^\dagger, R_1^\dagger, R_2^\dagger)$ is an achievable secrecy rate triple that lies *outside* the region $\mathcal{R}_{in}$. Since $(R_0^\dagger, R_1^\dagger, R_2^\dagger)$ is achievable, we can bound $R_0^\dagger$ by

$$R_0^\dagger \le \min\left(\frac{1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_1}{\mathbf{N}_1}\right|, \frac{1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_2}{\mathbf{N}_2}\right|\right) = R_0^{\max}.$$

Moreover, if $R_1^\dagger = R_2^\dagger = 0$, then $R_0^{\max}$ can be achieved by setting $\mathbf{B}_0 = \mathbf{S}$ and $\mathbf{B}_1 = 0$ in (6). Thus, we can find $\lambda_1 \ge 0$ and $\lambda_2 \ge 0$ such that

$$\lambda_1 R_1^\dagger + \lambda_2 R_2^\dagger = \lambda_1 R_1^\star + \lambda_2 R_2^\star + \rho \tag{10}$$

for some $\rho > 0$, where $\lambda_1 R_1^\star + \lambda_2 R_2^\star$ is given by

$$\begin{aligned} \max_{(\mathbf{B}_0,\,\mathbf{B}_1)} \quad & \lambda_1 f_1(\mathbf{B}_1) + \lambda_2 f_2(\mathbf{B}_0,\mathbf{B}_1) \\ \text{subject to} \quad & f_0(\mathbf{B}_0) \ge R_0^\dagger \\ & \mathbf{B}_0 \succeq 0 \\ & \mathbf{B}_1 \succeq 0 \\ & \mathbf{B}_0 + \mathbf{B}_1 \preceq \mathbf{S}. \end{aligned} \tag{11}$$

Let $(\mathbf{B}_0^\star, \mathbf{B}_1^\star)$ be an optimal solution to the above optimization program (11). Then, $(\mathbf{B}_0^\star, \mathbf{B}_1^\star)$ must satisfy the following Karush-Kuhn-Tucker (KKT) conditions:

$$(\beta_1+\lambda_2)[(\mathbf{S}-\mathbf{B}_0^\star)+\mathbf{N}_1]^{-1} + \beta_2[(\mathbf{S}-\mathbf{B}_0^\star)+\mathbf{N}_2]^{-1} + \mathbf{M}_0 = \lambda_2[(\mathbf{S}-\mathbf{B}_0^\star)+\mathbf{N}_2]^{-1} + \mathbf{M}_2 \tag{12}$$

$$(\lambda_1+\lambda_2)(\mathbf{B}_1^\star+\mathbf{N}_1)^{-1} + \mathbf{M}_1 = (\lambda_1+\lambda_2)(\mathbf{B}_1^\star+\mathbf{N}_2)^{-1} + \mathbf{M}_2 \tag{13}$$

$$\mathbf{M}_0\mathbf{B}_0^\star = 0,\ \mathbf{M}_1\mathbf{B}_1^\star = 0,\ \text{and}\ \mathbf{M}_2(\mathbf{S}-\mathbf{B}_0^\star-\mathbf{B}_1^\star) = 0 \tag{14}$$

where $\mathbf{M}_0$, $\mathbf{M}_1$ and $\mathbf{M}_2$ are positive semidefinite matrices, and β_k, $k=1,2$, is a nonnegative real scalar such that $\beta_k > 0$ if and only if

$$\frac{1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_k}{(\mathbf{S}-\mathbf{B}_0^\star)+\mathbf{N}_k}\right| = R_0^\dagger.$$

Hence, we have

$$\begin{aligned} &(\beta_1+\beta_2)R_0^\dagger + \lambda_1 R_1^\dagger + \lambda_2 R_2^\dagger \\ &= \frac{\beta_1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_1}{(\mathbf{S}-\mathbf{B}_0^\star)+\mathbf{N}_1}\right| + \frac{\beta_2}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_2}{(\mathbf{S}-\mathbf{B}_0^\star)+\mathbf{N}_2}\right| \\ &\quad + \lambda_1\left(\frac{1}{2}\log\left|\frac{\mathbf{B}_1^\star+\mathbf{N}_1}{\mathbf{N}_1}\right| - \frac{1}{2}\log\left|\frac{\mathbf{B}_1^\star+\mathbf{N}_2}{\mathbf{N}_2}\right|\right) \\ &\quad + \lambda_2\left(\frac{1}{2}\log\left|\frac{(\mathbf{S}-\mathbf{B}_0^\star)+\mathbf{N}_2}{\mathbf{B}_1^\star+\mathbf{N}_2}\right| - \frac{1}{2}\log\left|\frac{(\mathbf{S}-\mathbf{B}_0^\star)+\mathbf{N}_1}{\mathbf{B}_1^\star+\mathbf{N}_1}\right|\right) + \rho. \end{aligned} \tag{15}$$

Next, we shall find a contradiction to (15) by following the following three steps.

1) Step 1–Split Each Receiver into Two Virtual Receivers: Consider the following aligned MIMO Gaussian broadcast channel with four receivers:

$$\begin{aligned} \mathbf{Y}_{1a}[m] &= \mathbf{X}[m] + \mathbf{Z}_{1a}[m] \\ \mathbf{Y}_{1b}[m] &= \mathbf{X}[m] + \mathbf{Z}_{1b}[m] \\ \mathbf{Y}_{2a}[m] &= \mathbf{X}[m] + \mathbf{Z}_{2a}[m] \\ \text{and} \quad \mathbf{Y}_{2b}[m] &= \mathbf{X}[m] + \mathbf{Z}_{2b}[m] \end{aligned} \tag{16}$$

where $\{\mathbf{Z}_{1a}[m]\}$, $\{\mathbf{Z}_{1b}[m]\}$, $\{\mathbf{Z}_{2a}[m]\}$ and $\{\mathbf{Z}_{2b}[m]\}$ are i.i.d. additive vector Gaussian noise processes with zero means and covariance matrices $\mathbf{N}_1$, $\mathbf{N}_1$, $\mathbf{N}_2$ and $\mathbf{N}_2$, respectively. Suppose that the transmitter has three independent messages W_0, W_1 and W_2, where W_0 is intended for both receivers $1b$ and $2b$, W_1 is intended for receiver $1a$ but needs to be kept secret from receiver $2b$, and W_2 is intended for receiver $2a$ but needs to be kept secret from receiver $1b$. Note that the channel (16) has the same secrecy capacity region as the channel (5) under the same power constraints.

2) Step 2–Construct an Enhanced Channel: Let $\widetilde{\mathbf{N}}$ be a real symmetric matrix satisfying

$$\widetilde{\mathbf{N}} := \left(\mathbf{N}_1^{-1} + \frac{1}{\lambda_1+\lambda_2}\mathbf{M}_1\right)^{-1}. \tag{17}$$

Note that the above definition implies that $\widetilde{\mathbf{N}} \preceq \mathbf{N}_1$. Since $\mathbf{M}_1\mathbf{B}_1^\star = 0$, following [9, Lemma 11], we have

$$(\lambda_1+\lambda_2)(\mathbf{B}_1^\star+\widetilde{\mathbf{N}})^{-1} = (\lambda_1+\lambda_2)(\mathbf{B}_1^\star+\mathbf{N}_1)^{-1} + \mathbf{M}_1$$

and

$$|\mathbf{B}_1^\star+\widetilde{\mathbf{N}}||\mathbf{N}_1| = |\mathbf{B}_1^\star+\mathbf{N}_1|\,|\widetilde{\mathbf{N}}|. \tag{18}$$

Thus, by (13), we obtain

$$(\lambda_1+\lambda_2)(\mathbf{B}_1^\star+\widetilde{\mathbf{N}})^{-1} = (\lambda_1+\lambda_2)(\mathbf{B}_1^\star+\mathbf{N}_2)^{-1} + \mathbf{M}_2. \tag{19}$$

This implies that $\widetilde{\mathbf{N}} \preceq \mathbf{N}_2$. Consider the following enhanced aligned MIMO Gaussian broadcast channel

$$\begin{aligned} \widetilde{\mathbf{Y}}_{1a}[m] &= \mathbf{X}[m] + \widetilde{\mathbf{Z}}_{1a}[m] \\ \mathbf{Y}_{1b}[m] &= \mathbf{X}[m] + \mathbf{Z}_{1b}[m] \\ \widetilde{\mathbf{Y}}_{2a}[m] &= \mathbf{X}[m] + \widetilde{\mathbf{Z}}_{2a}[m] \\ \text{and} \qquad \mathbf{Y}_{2b}[m] &= \mathbf{X}[m] + \mathbf{Z}_{2b}[m] \end{aligned} \tag{20}$$

where $\{\widetilde{\mathbf{Z}}_{1a}[m]\}$, $\{\mathbf{Z}_{1b}[m]\}$, $\{\widetilde{\mathbf{Z}}_{2a}[m]\}$ and $\{\mathbf{Z}_{2b}[m]\}$ are i.i.d. additive vector Gaussian noise processes with zero means and covariance matrices $\widetilde{\mathbf{N}}$, $\mathbf{N}_1$, $\widetilde{\mathbf{N}}$ and $\mathbf{N}_2$, respectively. Since $\widetilde{\mathbf{N}} \preceq \{\mathbf{N}_1, \mathbf{N}_2\}$, we conclude that the secrecy capacity region of the channel (20) is at least as large as the secrecy capacity region of the channel (16) under the same power constraints.

Furthermore, based on (19), we have

$$\begin{aligned} &[(\mathbf{S} - \mathbf{B}_0^\star) + \widetilde{\mathbf{N}}](\mathbf{B}_1^\star + \widetilde{\mathbf{N}})^{-1} \\ &\qquad = [(\mathbf{S} - \mathbf{B}_0^\star) + \mathbf{N}_2](\mathbf{B}_1^\star + \mathbf{N}_2)^{-1} \end{aligned} \tag{21}$$

and hence,

$$\left| \frac{(\mathbf{S} - \mathbf{B}_0^\star) + \widetilde{\mathbf{N}}}{\mathbf{B}_1^\star + \widetilde{\mathbf{N}}} \right| = \left| \frac{(\mathbf{S} - \mathbf{B}_0^\star) + \mathbf{N}_2}{\mathbf{B}_1^\star + \mathbf{N}_2} \right|. \tag{22}$$

Combining (12) and (19), we may obtain

$$\begin{aligned} &(\lambda_1 + \lambda_2)[(\mathbf{S} - \mathbf{B}_0^\star) + \widetilde{\mathbf{N}}]^{-1} \\ &\quad = (\lambda_2 + \beta_1)[(\mathbf{S} - \mathbf{B}_0^\star) + \mathbf{N}_1]^{-1} \\ &\qquad + (\lambda_1 + \beta_2)[(\mathbf{S} - \mathbf{B}_0^\star) + \mathbf{N}_2]^{-1} + \mathbf{M}_0. \end{aligned} \tag{23}$$

Substituting (18) and (22) into (15), we have

$$\begin{aligned} &(\beta_1 + \beta_2)R_0^\dagger + \lambda_1 R_1^\dagger + \lambda_2 R_2^\dagger \\ &= \frac{\beta_1}{2} \log \left| \frac{\mathbf{S} + \mathbf{N}_1}{(\mathbf{S} - \mathbf{B}_0^\star) + \mathbf{N}_1} \right| + \frac{\beta_2}{2} \log \left| \frac{\mathbf{S} + \mathbf{N}_2}{(\mathbf{S} - \mathbf{B}_0^\star) + \mathbf{N}_2} \right| \\ &\quad + \lambda_1 \left(\frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0^\star) + \widetilde{\mathbf{N}}}{\widetilde{\mathbf{N}}} \right| - \frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0^\star) + \mathbf{N}_2}{\mathbf{N}_2} \right| \right) \\ &\quad + \lambda_2 \left(\frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0^\star) + \widetilde{\mathbf{N}}}{\widetilde{\mathbf{N}}} \right| - \frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0^\star) + \mathbf{N}_1}{\mathbf{N}_1} \right| \right) \\ &\quad + \rho. \end{aligned} \tag{24}$$

3) Step 3–Outer Bound for the Enhanced Channel: In the following, we shall consider a four-receiver discrete memoryless broadcast channel with a common message and two confidential messages and provide a single-letter outer bound on the secrecy capacity region.

Theorem 3 (Discrete memoryless broadcast channel): Consider a discrete memoryless broadcast channel with transition probability $p(\widetilde{\mathbf{y}}_{1a}, \mathbf{y}_{1b}, \widetilde{\mathbf{y}}_{2a}, \mathbf{y}_{2b}|\mathbf{x})$ and messages W_0 (intended for both receivers $1b$ and $2b$), W_1 (intended for receiver $1a$ but needing to be kept confidential from receiver $2b$) and W_2 (intended for receiver $2a$ but needing to be kept confidential from receiver $1b$). If both

$$\mathbf{X} \to \widetilde{\mathbf{Y}}_{1a} \to (\mathbf{Y}_{1b}, \mathbf{Y}_{2b}) \quad \text{and} \quad \mathbf{X} \to \widetilde{\mathbf{Y}}_{2a} \to (\mathbf{Y}_{1b}, \mathbf{Y}_{2b})$$

form Markov chains in their respective order, then the secrecy capacity region of this channel satisfies $\mathcal{C}_s^{[\mathrm{DMC}]} \subseteq \mathcal{R}_o$, where $\mathcal{R}_o$ denotes the set of nonnegative rate triples (R_0, R_1, R_2) such that

$$\begin{aligned} R_0 &\le \min[I(\mathbf{U}; \mathbf{Y}_{1b}),\ I(\mathbf{U}, \mathbf{Y}_{2b})] \\ R_1 &\le I(\mathbf{X}; \widetilde{\mathbf{Y}}_{1a}|\mathbf{U}) - I(\mathbf{X}; \mathbf{Y}_{2b}|\mathbf{U}) \\ \text{and} \qquad R_2 &\le I(\mathbf{X}; \widetilde{\mathbf{Y}}_{2a}|\mathbf{U}) - I(\mathbf{X}; \mathbf{Y}_{1b}|\mathbf{U}) \end{aligned} \tag{25}$$

for some $p(\mathbf{u}, \mathbf{x}) = p(\mathbf{u})p(\mathbf{x}|\mathbf{u})$.
The proof of Theorem 3 can be found in the extended version of this work [11].

Now, we may combine Steps 1, 2 and 3 and consider an upper bound on the weighted secrecy sum-capacity of the channel (5). By Theorem 3, for any achievable secrecy rate triple (R_0, R_1, R_2) for the channel (5) we have

$$\begin{aligned} &(\beta_1 + \beta_2)R_0 + \lambda_1 R_1 + \lambda_2 R_2 \\ &\quad \le \frac{\beta_1}{2} \log |2\pi e(\mathbf{S} + \mathbf{N}_1)| + \frac{\beta_2}{2} \log |2\pi e(\mathbf{S} + \mathbf{N}_2)| \\ &\qquad + \frac{\lambda_1}{2} \log \left| \frac{\mathbf{N}_2}{\widetilde{\mathbf{N}}} \right| + \frac{\lambda_2}{2} \log \left| \frac{\mathbf{N}_1}{\widetilde{\mathbf{N}}} \right| + \eta(\lambda_1, \lambda_2) \end{aligned} \tag{26}$$

where

$$\begin{aligned} \eta(\lambda_1, \lambda_2) &:= \lambda_1 h(\mathbf{X} + \widetilde{\mathbf{Z}}_{1a}|\mathbf{U}) + \lambda_2 h(\mathbf{X} + \widetilde{\mathbf{Z}}_{2a}|\mathbf{U}) \\ &\quad - (\lambda_2 + \beta_1) h(\mathbf{X} + \mathbf{Z}_{1b}|\mathbf{U}) - (\lambda_1 + \beta_2) h(\mathbf{X} + \mathbf{Z}_{2b}|\mathbf{U}). \end{aligned}$$

Note that $0 \prec \widetilde{\mathbf{N}} \preceq \{\mathbf{N}_1, \mathbf{N}_2\}$, $0 \prec \mathbf{B}_0^\star \preceq \mathbf{S}$ and $\mathbf{B}_0^\star \mathbf{M}_0 = 0$. Using [10, Corollary 4] and (23), we may obtain

$$\begin{aligned} \eta(\lambda_1, \lambda_2) &\le (\lambda_1 + \lambda_2) \log \left| 2\pi e(\mathbf{S} - \mathbf{B}_0^\star) + \widetilde{\mathbf{N}} \right| \\ &\quad - (\lambda_2 + \beta_1) \log |2\pi e(\mathbf{S} - \mathbf{B}_0^\star) + \mathbf{N}_1| \\ &\quad - (\lambda_1 + \beta_2) \log |2\pi e(\mathbf{S} - \mathbf{B}_0^\star) + \mathbf{N}_2|. \end{aligned} \tag{27}$$

Combining (26) and (27), for any achievable secrecy rate triple (R_0, R_1, R_2) for the channel (5) we have

$$\begin{aligned} &(\beta_1 + \beta_2)R_0 + \lambda_1 R_1 + \lambda_2 R_2 \\ &\le \frac{\beta_1}{2} \log \left| \frac{\mathbf{S} + \mathbf{N}_1}{(\mathbf{S} - \mathbf{B}_0^\star) + \mathbf{N}_1} \right| + \frac{\beta_2}{2} \log \left| \frac{\mathbf{S} + \mathbf{N}_2}{(\mathbf{S} - \mathbf{B}_0^\star) + \mathbf{N}_2} \right| \\ &\quad + \lambda_1 \left(\frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0^\star) + \widetilde{\mathbf{N}}}{\widetilde{\mathbf{N}}} \right| - \frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0^\star) + \mathbf{N}_2}{\mathbf{N}_2} \right| \right) \\ &\quad + \lambda_2 \left(\frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0^\star) + \widetilde{\mathbf{N}}}{\widetilde{\mathbf{N}}} \right| - \frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0^\star) + \mathbf{N}_1}{\mathbf{N}_1} \right| \right) \\ &< (\beta_1 + \beta_2)R_0^\dagger + \lambda_1 R_1^\dagger + \lambda_2 R_2^\dagger. \end{aligned} \tag{28}$$

Clearly, this contradicts the assumption that the rate triple $(R_0^\dagger, R_1^\dagger, R_2^\dagger)$ is achievable. Therefore, we have proved the desired converse result for Theorem 2.

IV. Numerical Example

In this section, we provide a numerical example to illustrate the secrecy capacity region of the MIMO Gaussian broadcast channel with a common message and two confidential messages. In this example, we assume that both the transmitter and each of the receivers are equipped with two antennas. The

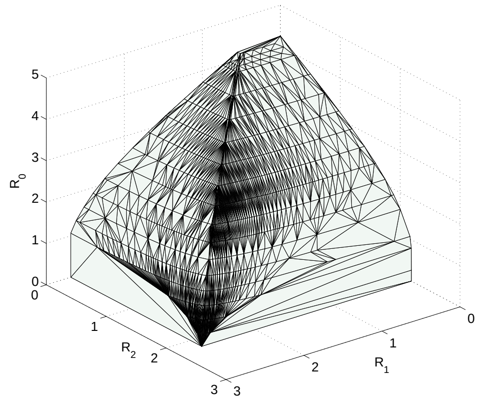

Fig. 2. Secrecy capacity region $\{(R_0, R_1, R_2)\}$

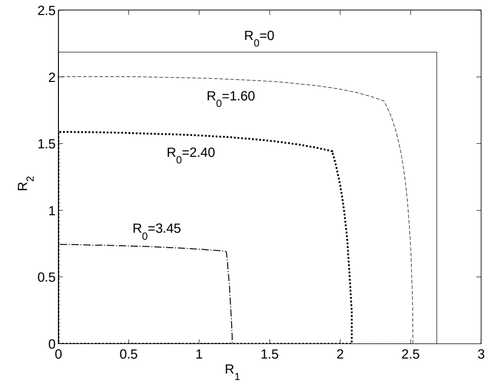

Fig. 3. Secrecy rate regions $\{(R_1, R_2)\}$ for some given R_0

channel matrices and the matrix power constraint are given by

$$\mathbf{H}_1 = \begin{pmatrix} 1.8 & 2.0 \\ 1.0 & 3.0 \end{pmatrix}, \ \mathbf{H}_2 = \begin{pmatrix} 3.3 & 1.3 \\ 2.0 & -1.5 \end{pmatrix}$$

$$\text{and} \qquad \mathbf{S} = \begin{pmatrix} 5.0 & 1.25 \\ 1.25 & 10.0 \end{pmatrix}.$$

which yield a *nondegraded* MIMO Gaussian broadcast channel. The boundary of the secrecy capacity region $\mathcal{C}_s^{[\mathrm{SBC}]}(\mathbf{H}_1, \mathbf{H}_2, \mathbf{S})$ is plotted in Fig. 2.

In Fig. 3, we have also plotted the boundaries of the secrecy capacity region (R_1, R_2) for some given common rate R_0. It is particularly worth mentioning that with $R_0 = 0$, the secrecy capacity region $\{(R_1, R_2)\}$ is *rectangular*, which implies that under the matrix power constraint, both confidential messages W_1 and W_2 can be simultaneously transmitted at their respective maximum secrecy rates. The readers are referred to [7] for further discussion of this phenomenon.

V. Conclusion

In this paper, we have considered the problem of communicating two confidential messages and a common message over a two-receiver MIMO Gaussian broadcast channel. We have shown that a natural scheme that combines secret dirty-paper coding and Gaussian superposition coding achieves the entire secrecy capacity region. To prove the converse result, we have applied a channel-enhancement argument and an extremal entropy inequality of Weingarten *et al.*, which generalizes the argument of [8] for the case with a common message and only one confidential message.

References

[1] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[2] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[3] R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz), "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, Article ID 370970, 8 pages, 2009.

[4] A. Khisti and G. W. Wornell, "The secrecy capacity of the MIMO wiretap channel," in *Proc. 45th Annual Allerton Conf. Comm., Contr., Computing*, Monticello, IL, Sep. 2007.

[5] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. Information Theory*, Toronto, Canada, July 2008, pp. 524–528.

[6] R. Liu and H. V. Poor, "Secrecy capacity region of a multi-antenna Gaussian broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1235–1249, Mar. 2009.

[7] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "Multiple-input multiple-output gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, submitted March 2009. [Online]. Available: http://arxiv.org/abs/0903.3786.

[8] H. D. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, submitted July 2009.

[9] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz), "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sep. 2006.

[10] H. Weingarten, T. Liu, S. Shamai (Shitz), Y. Steinberg, and P. Viswanath, "The capacity region of the degraded multiple-input multiple-output compound broadcast channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 5011–5023, Nov. 2009.

[11] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "MIMO Gaussian broadcast channels with confidential and common messages," *IEEE Trans. Inf. Theory*, submitted for publication.

[12] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4529–4542, Oct. 2009.